

**IN THE IN THE UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF OHIO**

UNITED STATE OF AMERICA,	)	<b>CASE NUMBER:</b> 1:16-cr-00270
	)	
Plaintiff,	)	<b>JUDGE:</b> SARA LIOI
	)	
vs.	)	
	)	
LAUDEN A. SULLIVAN,	)	
	)	
Defendant.	)	

**MOTION TO SUPPRESS**

Now comes the Defendant, by and through his undersigned counsel and moves this court pursuant to Fed. R. Crim. P. 12(b)(3)(c) for an order suppressing all evidence obtained from the Government’s deployment of a “Network Investigative Technique (hereinafter “NIT”),” used on Lauden Sullivan’s private computer. At all times relevant, Lauden Sullivan’s computer was located in Ohio.

All evidence obtained by the Government is the resulting fruits of the poisonous tree, stemming from its use of the NIT.

## STATEMENTS OF FACTS

The Government obtained evidence regarding Lauden Sullivan's alleged criminal activity via a multi-step process that began in the Autumn of 2014. At that time, Agents of the Federal Bureau of Investigation ("FBI") began investigating the Playpen Website ("Website A"), a global online forum believed to be hosting users for purposes of distributing and accessing child pornography.

The website's administrator was arrested in Naples, Florida in February of 2015. The FBI Agents took control of the site and instead of shutting it down, allowed it to operate for 12 days, from February 20, 2015 to March 4, 2015.

On February 20, 2015, the Government applied for and was granted a search warrant pursuant to Title III from a district judge in the eastern District of Virginia. The Title III warrant permitted the Government to intercept communications between the Playpen Website, identified in the warrant and here only as "Website A," and users via a "TOR" network.<sup>1</sup> Lauden Sullivan does not have, nor has he ever been presented with the Title III warrant.

On February 20, 2015, the Government also obtained a warrant from a magistrate judge in the Eastern District of Virginia to allow FBI Agents to covertly transmit computer code to users of Website A. (See Exhibit A "NIT Warrant" attached hereto). The request for the warrant was supported by an affidavit of Special Agent Douglas Macferlane wherein he states:

...the NIT may cause an activating computer - **wherever located** - to send to a computer controlled by or known by the government, network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer, as described above and in attachment B.

See Exhibit 1 pp 34 - 35. (Emphasis added)

---

<sup>1</sup>"TOR" stands for The Onion Router. It is a browser, similar to Safari or Google; however it is used to browse the hidden web.

The NIT warrant allowed the NIT software to obtain information from the users' computers and deliver it to the government. The information obtained included identifying information, including, but not limited to, the users' IP addresses, MAC addresses, type of operating system of the users' computer, the users' computers host name and the users' computer operating system username. Absent the use of the NIT, the Government had no ability to locate and identify users of Website A.

Once the Government had obtained the identification information outlined above, it used it to obtain a search warrants for individuals across the country, the "Residential Search warrants."

In this matter, FBI Agent Charles Sullivan, on January 19, 2016 applied for and was issued a residential search warrant, allowing the FBI to search and seize items located at 1216 West Jackson Street, Painesville, Ohio.

The residential Warrant was supported by the sworn affidavit of Agent Charles Sullivan. In the affidavit he states:

"Between February 20, 2015 and March 4, 2015 law enforcement agents acting pursuant to an order of the United States District Court for the Eastern District of Virginia monitored electronic communications of users of "Website A." (See Exhibit B, Affidavit of Sullivan p. 13).

He goes on, in his affidavit in support of the residential warrant application, to further detail what was gleaned from the NIT warrant and to indicate that utilization of the NIT was authorized by the NIT warrant.

"Pursuant to that authorization [of the Eastern District of Virginia], between February 20, 2015 and approximately March 4, 2015 each time any user or administrator logged into "Website A" by entering a username and password, the FBI was authorized to deploy the NIT which would send one or more communications to the user's computer. Those communications were designed to cause the receiving computer to deliver to a computer known to or controlled by the government data that would help identify the computer, its location, other information about the computer, and the user of the computer accessing "Website A."

(See Exhibit B paragraph 25, p 18).

The affidavit goes on to state that someone with username 554422 with IP address 76.188.24.146 accessed posts on March 1, 2015 and on March 4, 2015. *Id.* p.20. That on March 11, 2015 an administrative subpoena was served on Time Warner Cable requesting information for the user of IP address 76.188.24.146. *Id.* p.21.

Pursuant to the residential search warrant, agents searched and seized property belonging to Lauen Sullivan and others residing at 1216 West Jackson Street, Painesville Ohio in January of 2016. Mr. Sullivan was indicted on August 24, 2016 charged with two counts, to wit: Title 18 USC section 2256(a)(2) and 18 USC 2252A(a)(5)(B).

#### ARGUMENT

The Magistrate Judge who issued the NIT Warrant on February 20, 2015, had no authority to do so under the relevant statutory framework and Federal Rules as they existed on that date.

The issuance of the NIT warrant was contra to Fed. R. Crim. P. 41 and 28 U.S.C. section 636(a). A magistrate judge is only authorized to issue a search warrant for a location within the judicial district itself, with minor exceptions that are not applicable here.

Rule 41 (b), titled “Authority to Issue a Warrant,” provides:

At the request of a federal law enforcement officer or an attorney for the government:

(1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located **within the district**;

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district **if the person or property is located within the district when the warrant is issued** but might move or be moved outside the district before the warrant is executed;

(3) a magistrate judge— **in an investigation of domestic terrorism or international terrorism**—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

(4) a magistrate judge with authority in the district has authority to issue a warrant

to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located **within the district**, outside the district, or both; and

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, **but within any of the following**:

(A) a United States territory, possession, or commonwealth;

(B) the premises—no matter who owns them—of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or

land used for the mission's purposes; or

(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

Fed. R. Crim. P. 41(b).(Emphasis added).

The warrant in this case was not authorized under any of the applicable sections and is therefore void.<sup>2</sup> The results of the warrant must be suppressed.

The restriction is not a ministerial technicality. Rule 41 and section 636(a) serve as a critical line of protection against the extra territorial, international, searches that occurred in this case. Suppression of the evidenced seized (both in February and March of 2014 and the fruits of that seized evidence, the items and information seized from 1216 West Jackson Street, Painseville, Ohio) is mandated. A search warrant that the magistrate judge issued was not permitted by rule or statute to issue and is therefore void *ab initio*. See *States v. Master* 614 f.3d 236, 241 (6<sup>th</sup> Cir. 2010), *United States v. Peltier*, 344 F.Supp. 2d 539, 548 (E.D. Mich. 2004) (“A search warrant signed by a person who lacks the authority to issue it is void as a matter of law.”) (citation omitted); cf. *State v. Surowiecki*, 440 A.2d 798, 799 (Mont. 1981) (“[A] lawful signature on the search warrant by the person authorized to issue it [is] essential to its issuance[,]” such that an unsigned warrant is void

---

<sup>2</sup> The Federal Rules of Criminal Procedure were amended on December 1, 2016.

under state law and confers no authority to act, despite existence of probable cause). (See Exhibit C, Memorandum & Order U.S.A. v. Levin, 1:15-cr-10271-WGY Doc.69, attached hereto p. 19).

THE WARRANT IS NOT AUTHORIZED UNDER RULE 41(B)(1) AS IT EXISTED IN FEBRUARY OF 2015.

The rule was amended as of December 1, 2016. However, as it existed on February 20, 2015 Rule 41(b)(1) allowed a magistrate judge to issue a warrant for people or property located within that magistrate judge's district. The NIT Warrant inaccurately states that the evidence sought is "located in the Eastern District of Virginia." Attachment A to the NIT warrant indicates that the computer server, located in Virginia, is the place to be searched. (Exhibit A, attachment A). In reality, the "place to be searched" in this matter was 1216 West Jackson Street, Painesville, Ohio and the computer located in Painesville. Other courts have concluded that the computers to be searched were outside the jurisdiction of the Eastern District of Virginia. (See Exhibit C, U.S.A. v. Levin, pp. 12 - 13 wherein Judge Young conducts an analysis of the same NIT warrant utilized in this matter and cites to U.S. v. Michaud, 2016 WL 337263 (W.D. Wash. 2016)). The Levin court and the Michaud courts both found the argument that the crimes were committed within the location of Website A, Eastern District of Virginia, rather than on the personal computers located in other places under circumstances where users may have deliberately concealed their locations to be unpersuasive. Exhibit C pp. 12-13 and Michaud 2016 WL 337263 at \*6. See also In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013).

#### THE VIOLATION OF RULE 41 REQUIRES SUPPRESSION

The issuing magistrate judge herein lacked statutory authority to issue the NIT Warrant on February 20, 2014. Suppression is required as a violation of Rule 41 is also a violation of Section

636(a). See 28 U.S.C. 636(a). The territorial restrictions found in section 636(a) are jurisdictional limitations. “Section 636(a)’s territorial restrictions are **jurisdictional limitations** on the power of magistrate judges and the Supreme Court has long taught that the violation of a statutory jurisdictional limitation - quite unlike the violation of a more prosaic rule or statute - is *per se* harmful.” U.S. v. Krueger, 809 F. 3d at 1122 (emphasis added).

Violations of Rule 41 require suppression when a defendant is prejudiced by the lack of compliance. See United States v. Bonner, 808 F.2d 864, 869 (1<sup>st</sup> Cir 1986). “Prejudice means being ‘subjected to a search that might not have occurred or would not have been so abrasive’ had the rules been followed.” United States v. Burgos-Montes, 786 F.3d 92, 109 (1st Cir. 2015), quoting Bonner, 808 F.2d at 869. The case at bar stems from a scenario in which the voidable warrant resulted in prejudice and the collection of evidence that would not have been found if the rules would have been followed.

This violation of rule 41(b) is not the type of “ministerial” violation for which courts have declined to require suppression. Courts have suppressed the fruits of a Title III wiretap because the court had authorized the installation of a listening device outside its jurisdictional limits. The Court held that Rule 41(b), which partially implements Title III, is “crystal clear” and that “a jurisdictional flaw in the warrant” cannot be excused as a “technical defect.” United States v. Glover, 736 F.3d 509, at 515.

THE PARTICULARITY REQUIREMENT OF THE FOURTH AMENDMENT WAS VIOLATED.

The “manifest purpose of the particularity requirement of the Fourth Amendment is to prevent wide-ranging general searches by the police.” Bonner, 808 F.2d at 866. Here, the Government failed to comply with the Fourth Amendment’s particularity requirements. Had the

Government accurately described the place to be searched, ( a computer in painesville, Ohio), no warrant would have been issued. The search warrant erroneously described the place to be searched as the server, which purportedly had been moved by the government from North Carolina to Virginia.

It is evident from the plain language of Rule 41(b) that no interpretation would allow the search of potentially thousands of computers located across the globe and outside of the authorized district.

THE GOVERNMENT WAS AWARE AT THE TIME IT MADE APPLICATION FOR THE NIT WARRANT THAT IT WAS NOT AUTHORIZED.

The rule has since ben amended.<sup>3</sup> The amendment to Rule 41 with the addition of 41(b)(6)

---

<sup>3</sup>The pertinent amendments are as follows:

Rule 41. Search and Seizure

\* \* \* \* \*

(b) Venue for a Warrant Application.

At the request of a federal law enforcement officer or an attorney for the government:

\* \* \* \* \*

(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:

(A) the district where the media or information is located has been concealed through

technological means; or

(B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

\* \* \* \* \*

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

\* \* \* \* \*

(c) Receipt.

The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose



was first proposed in May of 2014. A memorandum addressed to the Committee on Rule of Practice and Procedure dated May 5, 2014, lays out with particularity the inherent problems for law enforcement complying with Rule 41 as it stood at that time. It also introduced a proposed amendment to Rule 41(b) that would authorize the use of the NIT Warrant. The proposed amendments were eventually adopted and made law on December 1, 2016. See Reena Raggi, Report of the Advisory Committee on Criminal Rules, May 5, 2014, at 484.<sup>4</sup> The memorandum states the reason for the proposal: stating that the **territorial venue provisions** create “special difficulties” for the Government when investigating crimes involving electronic information. *Id.* at 325. (Emphasis added).

The Government exceeded its jurisdiction and violated Lauden Sullivan’s Fourth Amendment rights when it executed the NIT warrant on February 20, 2014. The same warrant has been held by two other courts to be void *ab initio*. Exhibit C, Levin, Memorandum & Order, p. 19, (attached hereto) and United States v. Arterbury, No. 15 CR-182 (N.D. Okla. April 25, 2016)(Doc.27-8, pp. 16-17).

This case involves a violation of Rule 41(b), which is a substantive provision. It implicates substantive judicial authority. There is no Good-Faith Exception here, (For a complete analysis of

---

premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property. For a warrant to use remote access to search electronic storage media and seize or copy electronically stored information, the officer must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person.

\* \* \* \* \*

<sup>4</sup>Available at [http://www.uscourts.gov/sites/default/files/fr\\_import/ST2014-05.pdf](http://www.uscourts.gov/sites/default/files/fr_import/ST2014-05.pdf) pp. 484 - 485.

the Good -Faith exception as it applies to this warrant see attached Memorandum & Order, Levin, pp 24 - 34). Based upon the jurisdictional shortcomings of the warrant issued on February, 20, 2015 by the Magistrate Judge which resulted in the unlawful search of Lauden Sullivan's computer from February 20 to March 4, 2015, the evidence obtained at that time and from the Residential Warrant issued on January 19, 2016 must be suppressed.

### CONCLUSION

WHEREFORE, the defendant moves this Court for an order which suppresses all evidence obtained as a result of the February 20, 2015 NIT warrant and the Residential Warrant issued on January 19, 2016.

Respectfully submitted,

/s/ LOUIS J. CARLOZZI

**CARLOZZI & ASSOCIATES CO., L.P.A.**

BY: LOUIS J. CARLOZZI (#0062922)

Attorney for Defendant

1382 West 9<sup>th</sup> St., Suite 215

Cleveland, Ohio 44113

(216) 241-6277

(216) 241-6343 *fax*

lcarlozzi@sbcglobal.net

**SERVICE**

A copy of the foregoing Motion was forwarded by electronic mail via the clerks electronic filing system, and electronic mail to [Benedict.Gullo@usdoj.gov](mailto:Benedict.Gullo@usdoj.gov) Benedict S. Gullo, located at Office of the U.S. Attorney, Northern District of Ohio, Ste. 400, 801 Superior Ave., W. Cleveland, OH 44113, this 26 day of December, 2016.

*/LOUIS J. CARLOZZI*

**LOUIS J. CARLOZZI** (#0062922)  
Attorney for Defendant